PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-202436
(43)Date of publication of application : 27.07.2001

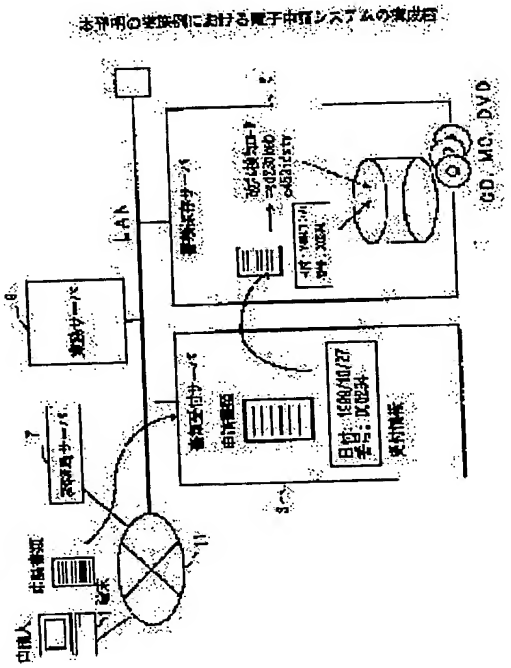
(51)Int.Cl. G06F 17/60
G06F 17/21
G09C 1/00
H04L 9/32

(21)Application number : 2000-011957
(22)Date of filing : 20.01.2000

(71)Applicant : RICOH CO LTD
(72)Inventor : KANAI YOICHI
YANAIDA MASUYOSHI

(54) ELECTRONIC APPLICATION SYSTEM, DOCUMENT STORAGE DEVICE, AND COMPUTER-READABLE RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic application system which secure the safety of a stored application document for a long period.
SOLUTION: The electronic application system is provided which permits application for an electronic document from a terminal through a network, and this electronic application system has a document storage device, a means for calculating an alteration detection code from information including a document sent from the terminal, and a means for storing the information in the document storage device together with the alteration detection code. The alteration detection code is a code calculated by using a secret key held in the document storage device. Further, the system has an update means for updating the secret key and an open key when the validity of the secret key expires, a means for calculating the alteration detection code held in the document storage device by using the updated secret key, and a means for using the alteration detection code as a new alteration detection code.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12)公開特許公報（A）

(11)特許出願公開番号

特開２００１－２０２４３６

（Ｐ２００１－２０２４３６Ａ）

(43)公開日　平成13年7月27日(2001.7.27)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	17/60		Ｇ０９Ｃ	1/00	６４０　Ｄ	5B009
	17/21				６４０　Ｂ	5B049
Ｇ０９Ｃ	1/00	６４０	Ｇ０６Ｆ	15/21	Ｚ	5J104
				15/20	５７０　Ｍ	9A001
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５　Ｄ	

審査請求　未請求　請求項の数１７　ＯＬ　（全１２頁）

(21)出願番号　特願2000-11957(P2000-11957)

(22)出願日　平成12年1月20日(2000.1.20)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込1丁目3番6号

(72)発明者　金井　洋一
東京都大田区中馬込1丁目3番6号　株式会社リコー内

(72)発明者　谷内田　益義
東京都大田区中馬込1丁目3番6号　株式会社リコー内

(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

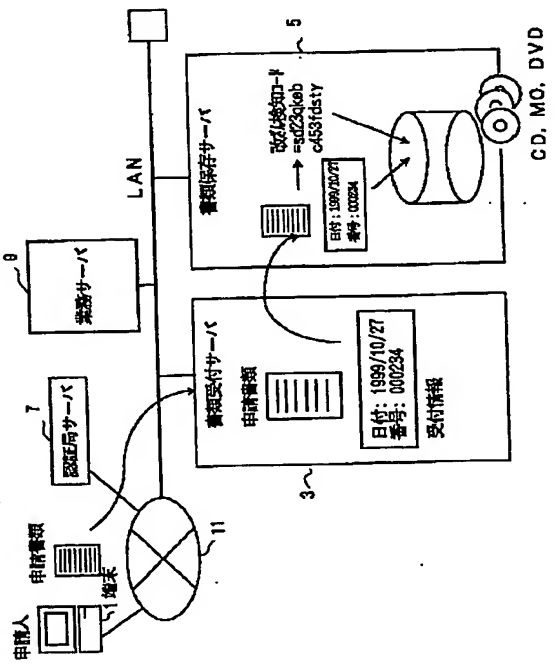
(54)【発明の名称】電子申請システム及び書類保存装置並びにコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】　保存された申請書類の安全性を長期にわたって確保する電子申請システムを提供することを目的とする。

【解決手段】　端末からネットワーク経由で電子的な書類の申請を行う電子申請システムが提供され、その電子申請システムは、書類保存装置と、端末から送信された書類を含む情報から改ざん検知コードを計算する手段と、該情報を該改ざん検知コードとともに書類保存装置に保存する手段とを有する。また、前記改ざん検知コードは、書類保存装置内に保持する秘密鍵を用いて計算したコードであり、前記秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手段と、更新された秘密鍵を用いて書類保存装置内に保持する改ざん検知コードを計算する手段と、該改ざん検知コードを新たな改ざん検知コードとして使用する手段とを更に有する。

本発明の実施例における電子申請システムの構成図



【特許請求の範囲】

【請求項１】　端末からネットワーク経由で電子的な書類の申請を行う電子申請システムであって、

書類保存装置と、

端末から送信された書類を含む情報から改ざん検知コードを計算する手段と、

該情報を該改ざん検知コードとともに書類保存装置に保存する手段とを有する電子申請システム。

【請求項２】　端末からネットワーク経由で電子的な書類の申請を行う電子申請システムであって、

書類保存装置と、

端末から送信された書類を受け付けた受付日時及び受付番号を含む受付情報を作成する手段と、

該書類と該受付情報とを含む情報から改ざん検知コードを計算する手段と、

該情報を該改ざん検知コードとともに書類保存装置に保存する手段とを有する電子申請システム。

【請求項３】　前記改ざん検知コードは、

書類保存装置内に保持する秘密鍵を用いて計算したコードである請求項１又は２に記載の電子申請システム。

【請求項４】　前記秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手段と、

更新された秘密鍵を用いて書類保存装置内に保持する改ざん検知コードを計算する手段と、

該改ざん検知コードを新たな改ざん検知コードとして使用する手段とを更に有する請求項３に記載の電子申請システム。

【請求項５】　オフライン記録媒体に書き出す書類のリストのリスト改ざん検知コードを作成する手段と、

該リストと、該リスト改ざん検知コードと、オフライン記録媒体の識別番号を書類保存装置に保存する手段と、

書き出し対象の書類を含む情報と、その情報の改ざん検知コードと、オフライン記録媒体の識別番号をオフライン記録媒体に書き出す手段を更に有する請求項１又は２に記載の電子申請システム。

【請求項６】　前記リスト改ざん検知コードは、書類保存装置内に保持する秘密鍵を用いて計算したコードであり、前記電子申請システムは、

秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手段と、

更新された秘密鍵を用いて書類保存装置内に保持する前記リストのリスト改ざん検知コードを計算する手段と、

新たに計算したリスト改ざん検知コードと、前記リストと、前記オフライン記録媒体の識別番号を書類保存装置に保存する手段とを更に有する請求項５に記載の電子申請システム。

【請求項７】　前記更新手段は、

書類保存装置に保持する公開鍵証明書を認証局に送信する手段と、

該公開鍵証明書に含まれる公開鍵により暗号化された鍵更新情報を受信する手段と、

該鍵更新情報を書類保存装置に保持する秘密鍵により復号し、新たな秘密鍵と新たな公開鍵証明書を取得する手段とを有する請求項４又は６に記載の電子申請システム。

【請求項８】　前記書類保存装置として原本性保証電子保存システムを用いる請求項１ないし７のうちいずれか1項に記載の電子申請システム。

【請求項９】　端末からネットワーク経由で電子的な書類の申請を行う電子申請システムにおける書類保存装置であって、

端末から送信された書類を含む情報から改ざん検知コードを計算する手段と、

該情報を該改ざん検知コードとともに保存する手段とを有する書類保存装置。

【請求項１０】　前記改ざん検知コードは、

書類保存装置内に保持する秘密鍵を用いて計算したコードである請求項９に記載の書類保存装置。

【請求項１１】　前記秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手段と、

更新された秘密鍵を用いて書類保存装置内に保持する改ざん検知コードを計算する手段と、

該改ざん検知コードを新たな改ざん検知コードとして使用する手段とを更に有する請求項１０に記載の書類保存装置。

【請求項１２】　端末からネットワーク経由で電子的な書類の申請を行い、書類保存装置を有する電子申請システム用のコンピュータ読み取り可能な記録媒体であって、

端末から送信された書類を含む情報から改ざん検知コードを計算する手順と、

該情報を該改ざん検知コードとともに書類保存装置に保存する手順とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１３】　端末からネットワーク経由で電子的な書類の申請を行い、書類保存装置を有する電子申請システム用のコンピュータ読み取り可能な記録媒体であって、

端末から送信された書類の受付日時及び受付番号を含む受付情報と該書類とを含む情報から改ざん検知コードを計算する手順と、

該情報を該改ざん検知コードとともに書類保存装置に保存する手順とをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１４】　前記改ざん検知コードは、

書類保存装置内に保持する秘密鍵を用いて計算したコードである請求項１２又は１３に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１５】　前記秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手順と、

更新された秘密鍵を用いて書類保存装置内に保持する改ざん検知コードを計算する手順と、
該改ざん検知コードを新たな改ざん検知コードとして使用する手順とを更にコンピュータに実行させる請求項１４に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項１６】　オフライン記録媒体に書き出す書類のリストのリスト改ざん検知コードを作成する手順と、
該リストと、該リスト改ざん検知コードと、オフライン記録媒体の識別番号を書類保存装置に保存する手順と、
書き出し対象の書類を含む情報と、その情報の改ざん検知コードと、オフライン記録媒体の識別番号をオフライン記録媒体に書き出す手順とを更にコンピュータに実行させる請求項１２又は１３に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項１７】　前記リスト改ざん検知コードは、書類保存装置内に保持する秘密鍵を用いて計算したコードであり、
秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手順と、
更新された秘密鍵を用いて書類保存装置内に保持する前記リストのリスト改ざん検知コードを計算する手順と、
新たに計算したリスト改ざん検知コードと、前記リストと、前記オフライン記録媒体の識別番号を書類保存装置に保存する手順とを更にコンピュータに実行させる請求項１６に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は電子文書の原本性を保証するための技術に関し、特に、申請人から受け付けた書類を保存する技術に関する。
【０００２】
【従来の技術】電子政府の実現に向けて様々な行政関連の申請手続きをインターネット経由で電子的に行うための実証実験が盛んに行われてきている。行政機関に対して申請された電子文書（申請書類）に対し、受け取った側の行政機関において、それを原本として扱うことができるようにするために、様々なセキュリティ技術が適用されている。
【０００３】電子申請を実現するシステムにおける従来技術として、例えば、特開平11－175607「書類送付システムおよび方法」に記載された技術では、代理人が作成した申請書類に対して、まず代理人が電子署名を付与し、更に申請人が支払い証明書を申請書類に付与した上で電子署名を付与する。そして、できあがった支払い証明書付き書類を書類受付サーバに送付し、書類受付サーバは受け付けた書類をデータベースに格納して管理するようにしている。
【０００４】この技術を利用することにより、インターネット経由で安全に申請書類を送付することができるようになっており、途中で申請書類に対して不正な改ざんなどが行われると、その改ざんを検出できる仕組みになっている。
【０００５】
【発明が解決しようとする課題】しかしながら、上記の従来の技術においては、改ざんを検出する仕組みは基本的にインターネット経由で書類をやり取りしている最中に重点をおいており、書類受付サーバ側で受け付けた後に書類が改ざんされてしまう可能性があることについては何ら対策を講じていない。
【０００６】インターネット上を申請書類が伝送されている時点では最適な暗号技術を利用して電子署名を施し、改ざんを検出できるようにしているため、伝送中の申請書類の安全性は確保されていると考えられる。しかし、書類受付サーバ側で書類を受け付けた後、その書類は例えば10年という長期間に渡って保存されることを考えると、長期にわたって受け付け書類の安全性を確保するには、申請人や代理人によって書類に付与された電子署名だけでは十分ではなく、後になって申請書類を改ざんできてしまう可能性があるという問題がある。すなわち、電子署名に用いられる暗号鍵の強度は一般的に時の経過とともに弱くなり、解読される可能性が高まるため、電子署名だけで書類を安全に長期間保存することは困難である。
【０００７】上述したように、申請人や代理人の電子署名を、書類作成の責任の所在を表す「印鑑」として扱うのは問題ないが、それを改ざん検知のためにも同時に利用してしまうという方針は長期にわたる安全性確保という観点からは望ましくない。
【０００８】本発明は上記の点に鑑みてなされたものであり、書類受付サーバ側において申請書類の安全性を長期にわたって確保する電子申請システムを提供することを目的とする。
【０００９】
【課題を解決するための手段】請求項１に記載の発明は、端末からネットワーク経由で電子的な書類の申請を行う電子申請システムであって、書類保存装置と、端末から送信された書類を含む情報から改ざん検知コードを計算する手段と、該情報を該改ざん検知コードとともに書類保存装置に保存する手段とを有する。
【００１０】従来技術では、電子署名の付いた書類を書誌事項を付してそのまま保存していあたため、例えば、署名に使用された秘密鍵の有効期限が切れた後は、書類の内容の原本性を保証することはできなかったが、本発明によれば、書類の保存の際に改ざん検知コードを付与するため、書類保存中の改ざんを検知することが可能となる。従って、長期間に亘って安全に書類を保存することが可能となり、長期に亘って保存書類の原本性を保証する電子申請システムを提供することが可能となる。

【００１１】請求項２に記載の発明は、端末からネットワーク経由で電子的な書類の申請を行う電子申請システムであって、書類保存装置と、端末から送信された書類を受け付けた受付日時及び受付番号を含む受付情報を作成する手段と、該書類と該受付情報とを含む情報から改ざん検知コードを計算する手段と、該情報を該改ざん検知コードとともに書類保存装置に保存する手段とを有する。

【００１２】本発明によれば、請求項１の発明と同様の作用効果を得ることができる。また、電子署名の付されていない受付情報も安全に保存できる。

【００１３】請求項３に記載の発明は、請求項１又は２の記載において、前記改ざん検知コードを書類保存装置内に保持する秘密鍵を用いて計算したコードであるとする。

【００１４】本発明によれば、従来の電子署名と同様な技術を使用して改ざん検知コードを付与することができる。

【００１５】請求項４に記載の発明は、請求項３の記載において、前記秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手段と、更新された秘密鍵を用いて書類保存装置内に保持する改ざん検知コードを計算する手段と、該改ざん検知コードを新たな改ざん検知コードとして使用する手段とを更に有することとする。

【００１６】本発明によれば、改ざん検知コードが自動的に更新されるため、長期に亘る書類の保存が可能となる。

【００１７】請求項５に記載の発明は、請求項１又は２の記載において、オフライン記録媒体に書き出す書類のリストのリスト改ざん検知コードを作成する手段と、該リストと、該リスト改ざん検知コードと、オフライン記録媒体の識別番号を書類保存装置に保存する手段と、書き出し対象の書類を含む情報と、その情報の改ざん検知コードと、オフライン記録媒体の識別番号をオフライン記録媒体に書き出す手段を更に有することとする。

【００１８】本発明によれば、後にオフライン記録媒体全体としての改ざん検知コードを更新することが可能となる。従って、このような保存手段を設けることによって、長期に亘る書類の保存に際し、受付書類の全てについて改ざん検知コードを更新する必要がなくなる。

【００１９】請求項６に記載の発明は、請求項５に記載において、前記リスト改ざん検知コードは、書類保存装置内に保持する秘密鍵を用いて計算したコードであり、前記電子申請システムは、秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手段と、更新された秘密鍵を用いて書類保存装置内に保持する前記リストのリスト改ざん検知コードを計算する手段と、新たに計算したリスト改ざん検知コードと、前記リストと、前記オフライン記録媒体の識別番号を書類保存装置に保存する手段とを更に有するとする。

【００２０】本発明によれば、オフライン記録媒体全体としての改ざん検知コードを更新することが可能となる。

【００２１】請求項７に記載の発明は、請求項4又は６の記載において、前記更新手段は、書類保存装置に保持する公開鍵証明書を認証局に送信する手段と、該公開鍵証明書に含まれる公開鍵により暗号化された鍵更新情報を受信する手段と、該鍵更新情報を書類保存装置に保持する秘密鍵により復号し、新たな秘密鍵と新たな公開鍵証明書を取得する手段とを有するものとする。

【００２２】本発明によれば、秘密鍵の更新を行うことが可能となる。

【００２３】請求項８に記載の発明は、請求項１ないし７のうちのいずれか1項の記載において、前記書類保存装置として原本性保証電子保存システムを用いることとする。

【００２４】原本性保証電子保存システムにおいては、ＣＰＵと記録媒体を物理的にパッケージ化した保存装置を用いて、電子原本の安全性を高めている。従って、本発明によれば、保存してある書類に対する外部からのアクセスが制限されるため、改ざんの脅威に対して更にセキュリティレベルが向上する。

【００２５】請求項９に記載の発明は、端末からネットワーク経由で電子的な書類の申請を行う電子申請システムにおける書類保存装置であって、端末から送信された書類を含む情報から改ざん検知コードを計算する手段と、該情報を該改ざん検知コードとともに保存する手段とを有する。

【００２６】本発明の書類保存装置を用いることによって、請求項１に記載の発明と同様の作用効果を得ることができる。

【００２７】請求項１０に記載の発明は、請求項９の記載において、前記改ざん検知コードは、書類保存装置内に保持する秘密鍵を用いて計算したコードであるとする。

【００２８】請求項１１に記載の発明は、請求項１０の記載において、前記秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手段と、更新された秘密鍵を用いて書類保存装置内に保持する改ざん検知コードを計算する手段と、該改ざん検知コードを新たな改ざん検知コードとして使用する手段とを更に有するとする。

【００２９】本発明は、請求項４に記載された発明と同様の作用効果を有する。

【００３０】請求項１２に記載の発明は、端末からネットワーク経由で電子的な書類の申請を行い、書類保存装置を有する電子申請システム用のコンピュータ読み取り可能な記録媒体であって、端末から送信された書類を含む情報から改ざん検知コードを計算する手順と、該情報を該改ざん検知コードとともに書類保存装置に保存する手順とをコンピュータに実行させるプログラムを記録す

る。本発明は、請求項１に記載された発明と同様の作用効果を有する。

【００３１】請求項１３に記載の発明は、端末からネットワーク経由で電子的な書類の申請を行い、書類保存装置を有する電子申請システム用のコンピュータ読み取り可能な記録媒体であって、端末から送信された書類の受付日時及び受付番号を含む受付情報と該書類とを含む情報から改ざん検知コードを計算する手順と、該情報を該改ざん検知コードとともに書類保存装置に保存する手順とをコンピュータに実行させるプログラムを記録する。本発明は、請求項２に記載された発明と同様の作用効果を有する。

【００３２】請求項１４に記載の発明は、請求項１２又は１３の記載において、前記改ざん検知コードは、書類保存装置内に保持する秘密鍵を用いて計算したコードであるとする。本発明は、請求項３に記載された発明と同様の作用効果を有する。

【００３３】請求項１５に記載の発明は、請求項１４の記載において、前記秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手順と、更新された秘密鍵を用いて書類保存装置内に保持する改ざん検知コードを計算する手順と、該改ざん検知コードを新たな改ざん検知コードとして使用する手順とを更にコンピュータに実行させるプログラムを記録する。本発明は、請求項４に記載された発明と同様の作用効果を有する。

【００３４】請求項１６に記載の発明は、請求項１２又は１３の記載において、オフライン記録媒体に書き出す書類のリストのリスト改ざん検知コードを作成する手順と、該リストと、該リスト改ざん検知コードと、オフライン記録媒体の識別番号を書類保存装置に保存する手順と、書き出し対象の書類を含む情報と、その情報の改ざん検知コードと、オフライン記録媒体の識別番号をオフライン記録媒体に書き出す手順とを更にコンピュータに実行させるプログラムを記録する。本発明は、請求項５に記載された発明と同様の作用効果を有する。

【００３５】請求項１７に記載の発明は、請求項１６の記載において、前記リスト改ざん検知コードは、書類保存装置内に保持する秘密鍵を用いて計算したコードであり、秘密鍵の有効期限が切れた場合に秘密鍵と公開鍵の更新を行う更新手順と、更新された秘密鍵を用いて書類保存装置内に保持する前記リストのリスト改ざん検知コードを計算する手順と、新たに計算したリスト改ざん検知コードと、前記リストと、前記オフライン記録媒体の識別番号を書類保存装置に保存する手順とを更にコンピュータに実行させるプログラムを記録する。本発明は、請求項６に記載された発明と同様の作用効果を有する。

【００３６】

【発明の実施の形態】以下、図を参照して本発明における実施例を説明する。図１は本発明の電子申請システムの構成図である。同図に示すように、本発明における電子申請システムは申請人の端末１、書類受付サーバ３、書類保存サーバ５、認証局サーバ７、業務サーバ９を有し、インターネット等のネットワーク１１を介して各装置は接続されている。書類受付サーバ３、書類保存サーバ５、及び業務サーバ９は例えば行政機関における業務システムを構成し、ＬＡＮにより接続されるが、書類受付サーバ３、書類保存サーバ５、及び業務サーバ９の各々がインターネット等の広域ネットワークに接続されていてもよい。認証局サーバ７はデジタル証明書の発行を行う第3者機関におけるサーバである。

【００３７】上記の構成において、端末１は申請人の作成した申請書類を書類受付サーバ３に送信する。書類受付サーバ３は申請書類を受け付け、書類保存サーバ５に保存したり、業務サーバ９に申請書類を送信する。書類保存サーバ５において書類の保存を行う。業務サーバ９は行政機関としての業務を行うためのサーバであり、例えば、住民票の処理等を行う。図１には、書類受付サーバ３と書類保存サーバ５を有する構成を示したが、書類保存サーバ５を備えず、書類受付サーバ３が書類保存も行うような構成としてもよい。この場合、書類受付サーバ３を書類保存サーバと称することができる。また、処理負荷や、求められる信頼性に応じて、書類受付サーバ３と書類保存サーバ５のそれぞれを複数台のサーバで構成することもできる。

【００３８】上述した書類保存サーバ５のハードウェア構成の一例を図２に示す。書類保存サーバ５は、ＣＰＵ（中央処理装置）１００、メモリ１０１、通信制御装置１０２、入力装置１０３、表示装置１０４、コンパクトディスク・ドライブユニット１０５、ハードディスク１０６を有する。ハードディスク１０６は書類保存サーバ５の外部装置として接続してもよいし、内部装置として有していてもよい。ＣＰＵ１００は書類保存サーバの全体を制御する。メモリ１０１はＣＰＵ１００で処理するデータやプログラムを保持する。通信制御装置１０２は書類保存サーバをＬＡＮ等のネットワークに接続するための制御を行う。入力装置１０３はキーボードやマウス等、データを入力する装置である。コンパクトディスク・ドライブユニット１０４はＣＤ－ＲＯＭ等を駆動し、読み書きを行う。本発明における後述する処理を実行するプログラムは、例えばＣＤ－ＲＯＭに格納され、コンパクトディスク・ドライブユニット１０４を介してハードディスク１０６にロードされる。プログラムが起動されると、所定のプログラム部分がメモリ１０１に展開され、処理が実行される。また、情報の保存のためのＭＯ（光磁気ディスク）ドライブやＤＶＤ（大容量光ディスク）ドライブを備えてもよい。ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等を書類保存サーバ５における記録媒体と称し、特に、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤについては書類保存サーバとはオフラインの状態で存在するので、オフライン記録媒体と称する。

【００３９】また、図３は書類保存サーバ５におけるソフトウェア構成の概略図である。ＯＳ１０７上に、書類保存アプリケーション１０８、他のアプリケーション１０９を有する構成をとる。書類保存アプリケーション１０８は、後述する書類保存処理、オフライン記録媒体への保存処理、改ざん検知コードの更新処理等を行い、他のアプリケーション１０９は、例えば、認証局との情報のやりとり等を行う。

【００４０】なお、本発明は書類保存サーバもしくは書類受付サーバ側での書類保存方法に特徴があるため、書類送付側の処理については概要のみを説明する。課金方法や代理人の取り扱いを含めたより実際的な方法については従来技術である特開平11－175607「書類送付システムおよび方法」などを参照されたい。

【００４１】以下、上記の電子申請システムにおける下記の処理に関する動作を説明する。

（１）書類送付・受付処理
（２）受付書類利用処理
（３）書類保存処理
（４）秘密鍵・公開鍵証明書更新処理
（５）既存受付書類の改ざん検知コード更新処理
（６）受付書類のオフライン記録媒体への書き出し処理
（７）オフライン記録媒体上の受付書類の改ざん検知コード更新処理

これらの処理は長期間の書類の保存を可能とするために必要な処理である。

【００４２】（１）書類送付・受付処理

まず、書類の送付・受付処理における動作を図４及び図５を用いて説明する。図４は書類の送付・受付処理におけるフローチャートであり、図５はその処理における申請書類、受付書類の構成を示す図である。（１）書類送付・受付処理の説明においては、書類受付サーバ３が書類を保存する例を用いる。

【００４３】ステップＳ１において申請人は申請のための書類１３を端末１において作成する。次に、ステップＳ２において、作成した書類に対して端末１は電子署名を計算し、その電子署名と書類をあわせて申請書類１５とする。そして、ステップＳ３として申請人は端末１からその申請書類１５を書類受付サーバ３に送付する。ステップＳ４では書類受付サーバ３が受け付けた申請書類１５に含まれている電子署名の正当性を確認する。ステップＳ４において電子署名が正しいことが確認されれば、ステップＳ５として書類受付サーバ３は受け付けた申請書類１５と、その受付日時や受付番号などの受付情報とを合わせて受付書類１７とする。

【００４４】ステップＳ６として書類受付サーバ３は自身が保有する秘密鍵を用いて、受付書類に対する改ざん検知コードを計算し、ステップＳ７としてその改ざん検知コード１９を受付書類１７とともに書類受付サーバ３が有する受付書類データベースに格納する。上記の改ざん検知コードは、保存書類の改ざんを検知するためのコードであり、次のようにして求められる。すなわち、まず、受付書類に対して一方向関数を適用して圧縮データを作成し、その圧縮データを、書類保存サーバ内部に保持している秘密鍵で暗号化する。なお、改ざん検知コードの取得方法は、従来の電子署名の取得方法と同様である。

【００４５】このように、受付日時や受付番号などの受付情報（書誌事項とも称される）と書類を合わせたものを暗号化するため、電子署名が付されていない書誌事項だけが改ざんされるようなことが防止できる。

【００４６】（２）受付書類利用処理

次に、書類受付サーバ３における受付書類データベースに格納された受付書類を後で業務サーバ９が利用する際における処理を図６のフローチャートを用いて説明する。

【００４７】最初に、ステップＳ１１として業務サーバ９は処理する受付書類とその改ざん検知コードを受付書類データベースから取得し、ステップＳ１２にて改ざん検知コードの正当性を確認する。必要であればステップＳ１３として受付書類に含まれる申請書類に含まれている電子署名の正当性を確認する。そして、正当性の確認された受付書類を利用する（ステップＳ１４）。

【００４８】上述の通り、書類受付サーバ３が計算して付与した改ざん検知コードは誰かの印鑑の役割を果たしているのではなく、書類の改ざんを検知するために付与される。従って、長期にわたって受付書類を保存しなければならない場合には、その改ざん検知コードを定期的に例えば別の秘密鍵を使用した改ざん検知コードに付け替えたり、新しい改ざん検知アルゴリズムを使用した改ざん検知コードに付け替えることにより効果的に改ざんを防止できる。

【００４９】このような長期に渡って安全性を確保する機能は、上記の書類受付サーバ３もしくは書類保存サーバ５のどちらに設けても良いが、以降の説明においては書類保存サーバ５が書類を長期に渡って安全に保存する機能を有するものとする。

【００５０】なお、改ざん検知コードの付与には秘密鍵を使用するため、書類保存サーバ５のような書類保存専用のサーバを設けることがセキュリティ上好ましい。

【００５１】（３）書類保存処理

書類保存サーバ５が、書類受付サーバ３が受付けた書類を保存する場合の動作について図７のフローチャートを参照して説明する。書類保存サーバ５が下記の処理を行う場合、書類受付サーバ３は書類の受付処理を行うだけであり、書類受付サーバ３は上記の書類送付・受付処理のステップＳ５までを行った後、受付書類を書類保存サーバ５に渡すこととなる。

【００５２】ステップＳ２１として書類保存サーバ５は書類受付サーバ３から受付書類を受け取る。そして、ス

テップＳ２２として受付書類に対して一方向関数を適用して圧縮データを作成し、ステップＳ２３において、その圧縮データを、書類保存サーバ５内部に保持している秘密鍵で暗号化し、上述した改ざん検知コードとする。ステップＳ２４として、その改ざん検知コードと受付書類と書類保存サーバの公開鍵証明書を書類保存サーバ５の記録媒体に保存する。

【００５３】（４）秘密鍵・公開鍵証明書更新処理

上記の書類保存サーバ５内部に保持している秘密鍵と公開鍵証明書には一般的に有効期限が設定されている。有効期限が切れた場合に、その秘密鍵と公開鍵証明書を書類保存サーバ管理者が手動で更新しても良いが、自動的に更新するようにしても良い。自動的に更新することによって確実に更新を行うことが可能となる。これにより書類を安全に長期間保存することが可能となる。

【００５４】自動的に更新する場合の処理について図８のフローチャートを用いて説明する。図８に示す秘密鍵・公開鍵証明書更新処理を実行するタイミングは、前記書類保存処理におけるステップＳ２１の直後に毎回実行しても良いし、日々既定の時刻に実行するようにスケジュールしても良い。

【００５５】まず、ステップＳ３１として書類保存サーバ５は内部に保持している公開鍵証明書に記載されている有効期限を読み取り、有効期限が切れていなければ終了（ステップＳ３２、ステップＳ３３）する。有効期限が切れている場合には、新規に秘密鍵と公開鍵の組を生成する（ステップＳ３２、ステップＳ３４）。

【００５６】次に、ステップＳ３５として、生成した公開鍵を、書類保存サーバ５内に保持している既存の公開鍵証明書とともに認証局サーバ７に送付する。ステップＳ３６として認証局サーバ７内では、受け取った公開鍵証明書の正当性を確認し、正当性が確認されたらステップＳ３７にて新しい公開鍵に対して認証局としての証明書を作成し、ステップＳ３８として、作成された新しい公開鍵証明書を、先に受け取った公開鍵証明書に含まれる公開鍵で暗号化する。これは、もともとの公開鍵証明書の持ち主に新しい公開鍵証明書が送られるようにするために行われる。そして、暗号化した新しい公開鍵証明書を、書類保存サーバ５に返送する（ステップＳ３９）。なお、公開鍵証明書とは、公開鍵とそれがだれのものかを示す属性情報とを合わせた情報に署名を付したものであり、公開鍵証明書の正当性を確認することは、その署名の正当性を確認することに相当する。

【００５７】ステップＳ４０として、書類保存サーバ５は、受け取った暗号化された新しい公開鍵証明書を、書類保存サーバ５内部に保持している既存の秘密鍵で復号し、ステップＳ４１として復号して得られた公開鍵証明書を新しい公開鍵証明書、先に生成した秘密鍵を新しい秘密鍵として書類保存サーバ５内部に保持する。

【００５８】このような処理を行うことによって、次に書類受付サーバ３に送付された申請書類からは新しい秘密鍵を使用して改ざん検知コードを計算するようになる。

【００５９】（５）既存受付書類の改ざん検知コード更新処理

上記の処理を行っても、以前に受け付けて書類保存サーバ５においてすでに保存している受付書類については改ざん検出コードが更新されない。そこで、すでに保存している受付書類の改ざん検出コードを更新することによってより効果的に改ざんを防止することが可能となる。その例について図９のフローチャートを用いて次に説明する。以下の説明においては、上述のようにして更新した秘密鍵、公開鍵、公開鍵証明書のことを新秘密鍵、新公開鍵、新公開鍵証明書と称し、更新前のものを旧秘密鍵、旧公開鍵、旧公開鍵証明書と称する。

【００６０】ステップＳ５１として、書類保存サーバ５は、内部に保存している既存の受付書類と、それとともに保存されている改ざん検知コードを読み出し、ステップＳ５２として、既存の受付書類に対して一方向関数を適用して圧縮データを作成する。そして、ステップＳ５３として先に読み出した改ざん検知コードを、旧公開鍵証明書に含まれる旧公開鍵で復号し、ステップＳ５４として、その復号した改ざん検知コードが先の圧縮データと一致するかどうか検査する。一致しなければ既存の受付書類はすでに改ざんされているものとしてエラー終了する（ステップＳ５５、ステップＳ５６）。

【００６１】一致していれば、先に計算した圧縮データを、新秘密鍵により暗号化して改ざん検知コードとし（ステップＳ５５、ステップＳ５７）、その改ざん検知コードと新公開鍵証明書とを、対象とした既存の受付書類とともに書類保存サーバ内部に保存する（ステップＳ５８）。

【００６２】具体的にはすべての既存の受付書類に対して上記処理を繰り返すことになる。この処理は秘密鍵・公開鍵証明書更新処理の直後に行っても良いが、受付書類が大量になると非常に処理に時間がかかることが予想されるため、例えば夜間の決められた時間に処理を行うようにスケジュールしても良い。

【００６３】（６）受付書類のオフライン記録媒体への書き出し処理

受付書類が更に大量になると、例えばＣＤ－ＲＯＭやＭＯ、ＤＶＤといったオフラインの記録媒体に受付書類を記録する。そのような場合に、オフラインの記録媒体に保存されているすべての受付書類の改ざん検知コードを更新することは現実的でない。そこで、受付書類をオフライン記録媒体に保存する場合には以下のように処理することができる。

【００６４】書類保存サーバ５内部に保存されている受付書類を複数一括してオフライン記録媒体に書き出す処理について図１０のフローチャートを用いて説明する。

また、図１１に上記の処理における各データの具体例を示す。

【００６５】ステップＳ６１として、書類保存サーバ５は、書類保存サーバ５内に保存されている受付書類の中で、オフライン記録媒体に書き出す受付書類のリスト２１を作成する。図１１に示すように、リストの各要素には受付書類名と受付書類とともに保存されている改ざん検知コードを含む。次に、ステップＳ６２として、作成したリストに一方向関数を適用して圧縮データ２３を作成し、ステップＳ６３にて、その圧縮データ２３を書類保存サーバ５内に保持している秘密鍵で暗号化し、リスト改ざん検知コード２５とする。

【００６６】次に、ステップＳ６４として、オフライン記録媒体に固有のオフライン記録媒体識別番号２７を生成し、ステップＳ６５において、作成したオフライン記録媒体書き出しリスト２１、リスト改ざん検知コード２５、オフライン記録媒体識別番号２７を合わせてオフライン記録媒体管理情報２９とする。そのオフライン記録媒体管理情報２９を書類保存サーバ５内に保存する（ステップＳ６６）。ステップＳ６７として、書類保存サーバ５は、書き出し対象となった受付書類とその受付書類の改ざん検知コード、オフライン記録媒体識別番号をオフライン記録媒体に書き出す。

【００６７】（７）オフライン記録媒体上の受付書類の改ざん検知コード更新処理

上記のようにして書き出されたオフライン記録媒体上の受付書類について、後に書類保存サーバ５の秘密鍵、公開鍵証明書を更新した際には、図１２のフローチャートに示すような改ざん検知コード更新処理を行う。

【００６８】ステップＳ７１として、書類保存サーバ５は、内部に記録しているオフライン記録媒体管理情報２９を読み出し、ステップＳ７２として、オフライン記録媒体管理情報２９からオフライン記録媒体書き出しリスト２１、リスト改ざん検知コード２５、オフライン記録媒体識別番号２７を取り出す。次に、ステップＳ７３としてオフライン記録媒体書き出しリスト２１に一方向関数を適用して圧縮データを作成する。また、ステップＳ７４として、リスト改ざん検知コード２５を書類保存サーバの旧公開鍵証明書に含まれる旧公開鍵を用いて復号する。

【００６９】ステップＳ７５において、復号したリスト改ざん検知コードが先の圧縮データと一致するかどうか検査する。一致しなければすでにオフライン記録媒体書き出しリスト２１が改ざんされているものとしてエラー終了し（ステップＳ７６、ステップＳ７７）、一致していれば、先の圧縮データを新秘密鍵で暗号化し、新しいリスト改ざん検知コードとする（ステップＳ７６、ステップＳ７８）。そして、ステップＳ７９において、新しいリスト改ざん検知コードと、先のオフライン記録媒体書き出しリスト２１、オフライン記録媒体識別番号を合わせて新しいオフライン記録媒体管理情報とし、新しいオフライン記録媒体情報を書類保存サーバ５内に保存する（ステップＳ８０）。

【００７０】上記の処理を、書類保存サーバ５内部に記録しているオフライン記録媒体管理情報ごとに実行することになる。

【００７１】上記の処理においては、オフライン記録媒体上の受付書類すべてについて改ざん検知コードを更新せずとも、オフライン記録媒体全体としての改ざん検知コードを更新することで、長期間に渡る安全性を確保するようにしている。

【００７２】一方向関数を適用したときに、もともとの受付書類と同じ圧縮データを生成するような、意味のある別の文書を作成されてしまうリスクは低く、むしろ、複数の受付書類に付与されている改ざん検知コードを集めてくることでその改ざん検知コードを生成する際に使用した秘密鍵が解読されるリスクが高いということが脅威として想定されるため、上記の処理が有効である。

【００７３】上記の書類保存サーバ５は、以下の（１）～（４）の文献に示す従来技術における原本性保証電子保存システムを適用することによって実現するようにしても良い。原本性保証電子保存システムにおいては、ＣＰＵと記録媒体を物理的にパッケージ化した保存装置を用いて、電子原本の安全性を高めている。原本性保証電子保存システムを適用すれば、原本性保証電子保存システム内部に保存してある書類に対する外部からのアクセスが制限されるため、改ざんの脅威に対して更にセキュリティレベルが向上する。

（１）小尾他：原本性保証電子保存システムの開発－基本機能の実現、MedicalImaging Technology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting '98(1998)

（２）金井他：原本性保証電子保存システムの開発－システムの構築－, Medical Imaging Technology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)

（３）国分他：原本性保証電子保存システムの開発、（特）情報処理振興事業協会発行　創造的ソフトウェア育成事業及びエレクトロニック・コマース推進事業最終成果発表会論文集　創造的ソフトウェア育成事業編（１９９８）

（４）金井：原本性保証電子保存システムについて, Vol.34, No.8, 行政＆ＡＤＰ（１９９８）

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。例えば、上記の実施例では、改ざん検知コードを電子署名の手法を用いて付与したが、電子公証情報を改ざん検知コードとして使用することも可能である。

【００７４】

【発明の効果】本発明によれば、申請書類と書誌事項とを合わせた情報に改ざん検知コードを付与して保存し、

その改ざん検知コードを更新することができるので、書類受付サーバで受け付けた申請書類を長期に渡って安全に保存することが可能になる。それにより、電子政府に必要不可欠となる電子申請システムの構築が実現できることとなる。

【図面の簡単な説明】

【図１】本発明の実施例における電子申請システムの構成図である。

【図２】書類保存サーバ５のハードウェア構成の一例を示す図である。

【図３】書類保存サーバ５におけるソフトウェア構成の概略図である。

【図４】書類の送付・受付処理の流れを示すフローチャートである。

【図５】書類の送付・受付処理における申請書類、受付書類の構成を示す図である。

【図６】受付書類利用処理の流れを示すフローチャートである。

【図７】書類保存処理の流れを示すフローチャートである。

【図８】秘密鍵・公開鍵証明書更新処理の流れを示すフローチャートである。

【図９】既存受付書類の改ざん検知コード更新処理の流れを示すフローチャートである。

【図１０】受付書類のオフライン記録媒体への書き出し処理の流れを示すフローチャートである。

【図１１】受付書類のオフライン記録媒体への書き出し処理における各データの具体例を示す図である。

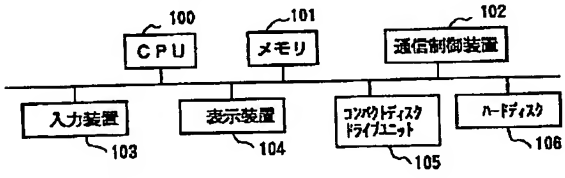
【図１２】オフライン記録媒体上の受付書類の改ざん検知コード更新処理の流れを示すフローチャートである。

【符号の説明】

１　端末
３　書類受付サーバ
５　書類保存サーバ
７　認証局サーバ
９　業務サーバ
１１　ネットワーク
１３　書類
１５　申請書類
１７　受付書類
１９　改ざん検知コード
２１　オフライン記録媒体に書き出す受付書類のリスト
２３　圧縮データ
２５　リスト改ざん検知コード
２７　オフライン記録媒体識別番号
２９　オフライン記録媒体管理情報
１００　ＣＰＵ（中央処理装置）
１０１　メモリ
１０２　通信制御装置
１０３　入力装置
１０４　表示装置
１０５　コンパクトディスク・ドライブユニット
１０６　ハードディスク
１０７　ＯＳ（オペレーティングシステム）
１０８　書類保存アプリケーション
１０９　他のアプリケーション

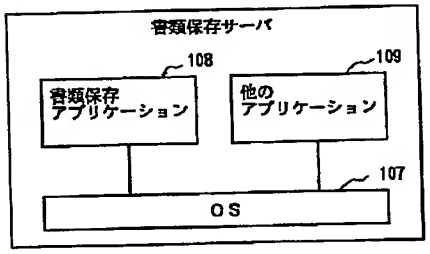
【図２】

書類保存サーバ５のハードウェア構成の一例を示す図



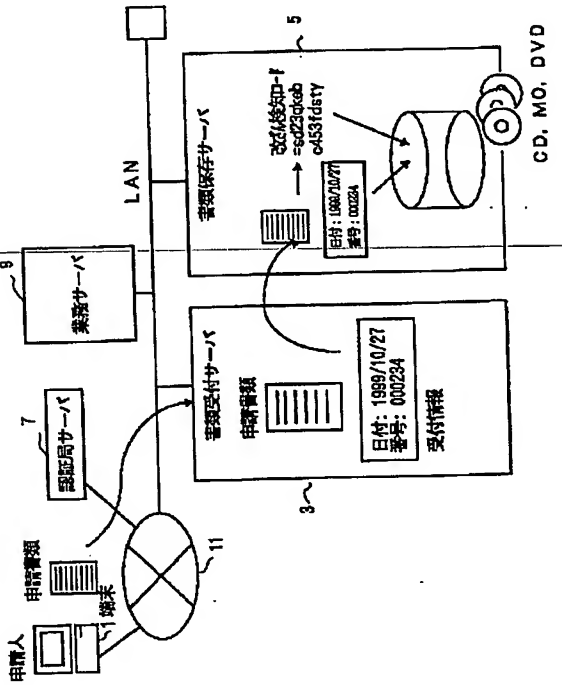
【図３】

書類保存サーバ５におけるソフトウェア構成の概略図



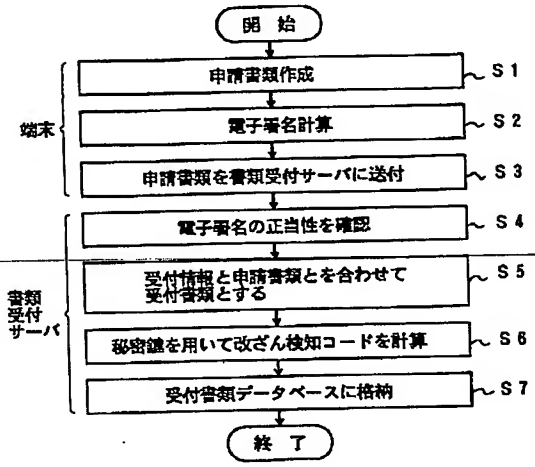
【図１】

本発明の実施例における電子申請システムの構成図



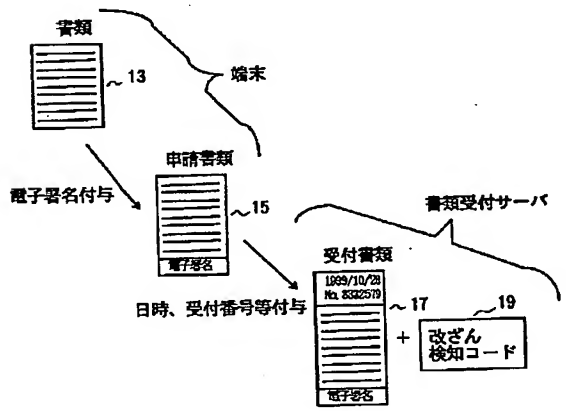
【図４】

書類の送付・受付処理の流れを示すフローチャート



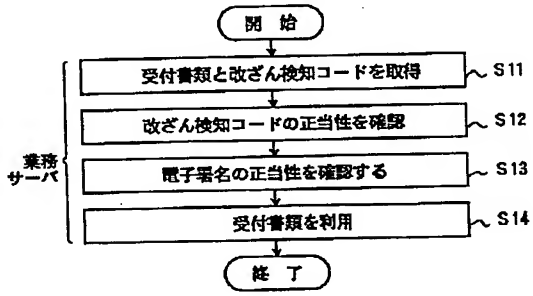
【図５】

書類の送付・受付処理における申請書類、受付書類の構成を示す図



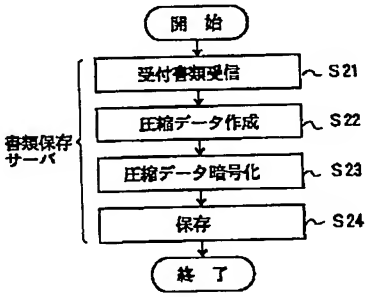
【図６】

受付書類利用処理の流れを示すフローチャート



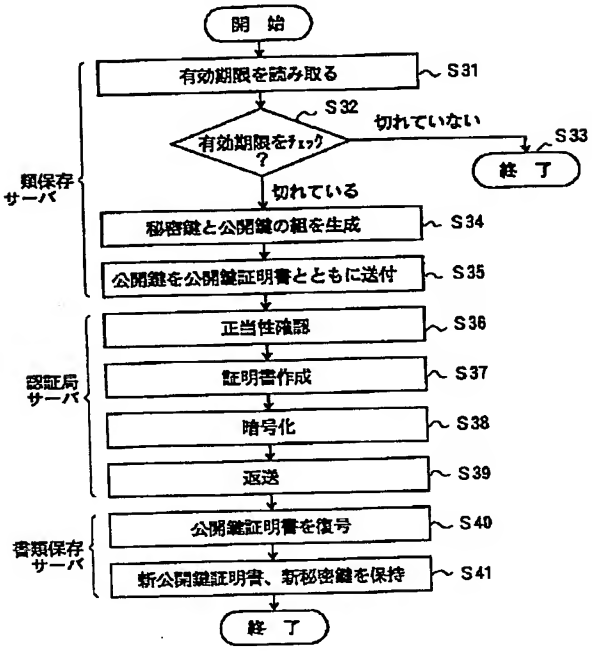
【図７】

書類保存処理の流れを示すフローチャート



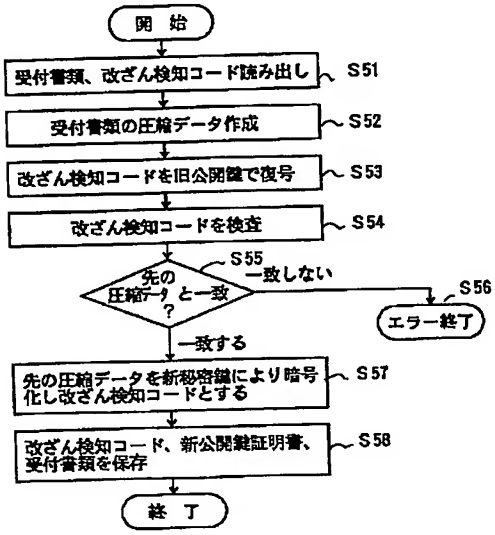
【図８】

秘密鍵・公開鍵証明書更新処理の流れを示すフローチャート



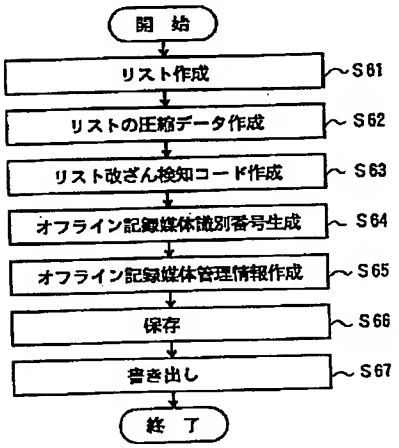
【図９】

既存受付書類の改ざん検知コード更新処理の流れを示すフローチャート



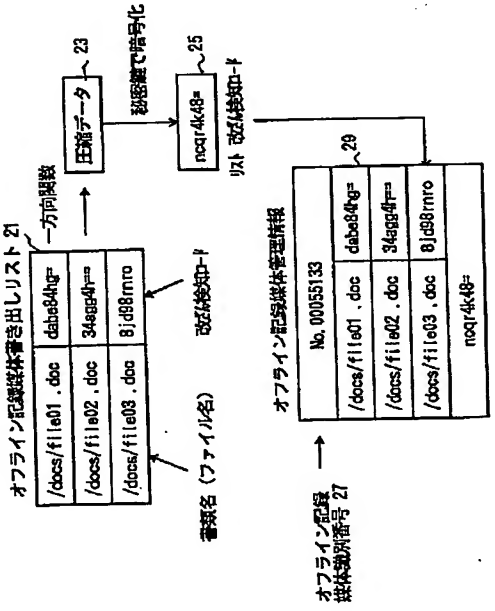
【図１０】

受付書類のオフライン記録媒体への書き出し処理の流れを示すフローチャート



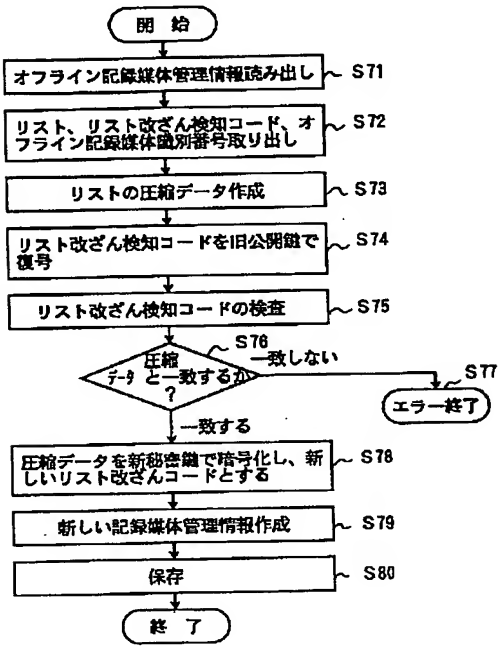
【図１１】

受付書類のオフライン記録媒体への書き出し処理における各データの具体例を示す図



【図１２】

オフライン記録媒体上の受付書類の改ざん検知コード更新処理の流れを示すフローチャート



フロントページの続き

Ｆターム(参考)　5B009 SA14 TB13
5B049 AA01 AA02 AA05 CC00 CC01
EE01 FF09 GG04 GG07 GG10
5J104 AA08 AA11 AA34 JA21 LA03
MA02 NA02 NA27 PA07 PA13
9A001 EE03 JJ07 JJ34 LL03